IT@UMN
INFORMATION TECHNOLOGY

University Information Security Awareness

Stay Safe Online!

Jenny Blaine
University Information Security

University of Minnesota

IT@UMN

June 2017

Your accounts and identity are valuable > you have valuable access, assets, and trust relationships

http://phishing.it.umn.edu/2014/07/whats-your-email-worth.html

Threats - What the cyber criminals are doing

- **Fraudulent email and other scams** -> try to trick you into logging in or otherwise revealing your ID and password - can be highly targeted or a random spamming event - can also trick you into installing malware

- **Malware** -> infect your computer and transfer your information > attachments or infected websites can be vectors

- **Ransomware** -> malware that encrypts your files and the files of any shared drives mapped on your computer and holds them for ransom until you pay; dangerous to pay

- **Malicious websites or ads on websites** -> distribute malware or compromise your credentials
  - Use Ad Aware AdBlock or McAfee SiteAdvisor
  - Use UMN VPN to protect your wireless traffic > **safecomputing.umn.edu**

IT@UMN

OneClass - Note Taking App

- *Spreads by phishing*
- *Malicious browser plugin appears to be legit*
- *Teachers may not know it's there*
- *Against student conduct code*

WEDNESDAY, JANUARY 25, 2017

Security Advisory: Malicious Chrome Extension

SECURITY ADVISORY: MALICIOUS CHROME EXTENSION

Tuesday, December 20, 2016

A Chrome Extension, OneClass, is part of an unauthorized application that could affect your Canvas account. If installed, OneClass may masquerade as you to send email and attempt to collect your login credentials.

The OneClass Extension is not available directly in the Chrome Extensions Store but students at other institutions are being phished with an installation link in direct email messages. During installation, the extension requests permissions to "Read and change all your data on the websites you visit." Although OneClass is not affiliated with Canvas, when users install the browser extension, it displays a button in the browser window encouraging the user to "Invite Your Classmates to OneClass." If clicked, OneClass will use Canvas's Conversations tool ("Inbox") to email all the users in your courses and phish them to install the extension, too, using the following message:

"Hey guys, I just found some really helpful notes for the upcoming exams for University of Minnesota courses at <URL>. I highly recommend signing up for an account now that way your first download is free!"

Please **DO NOT** install this extension, and if you receive an email like the one above DO NOT click anything in the email, just delete the message. If you have already installed the OneClass extension in Chrome, please uninstall it immediately (for information on how to remove Chrome extensions, see the "Uninstall an extension" section in the document: https://support.google.com/chrome_webstore/answer/2664769).

We will continue to monitor this issue and provide updates to you as new information becomes available.

Why?

IT@UMN

June 2017

You have the power to protect yourself and the University!
UMN two-factor protection in front of W2 & Direct Deposit protects your financial information.

- https://it.umn.edu/duo-set-two-factor-authentication

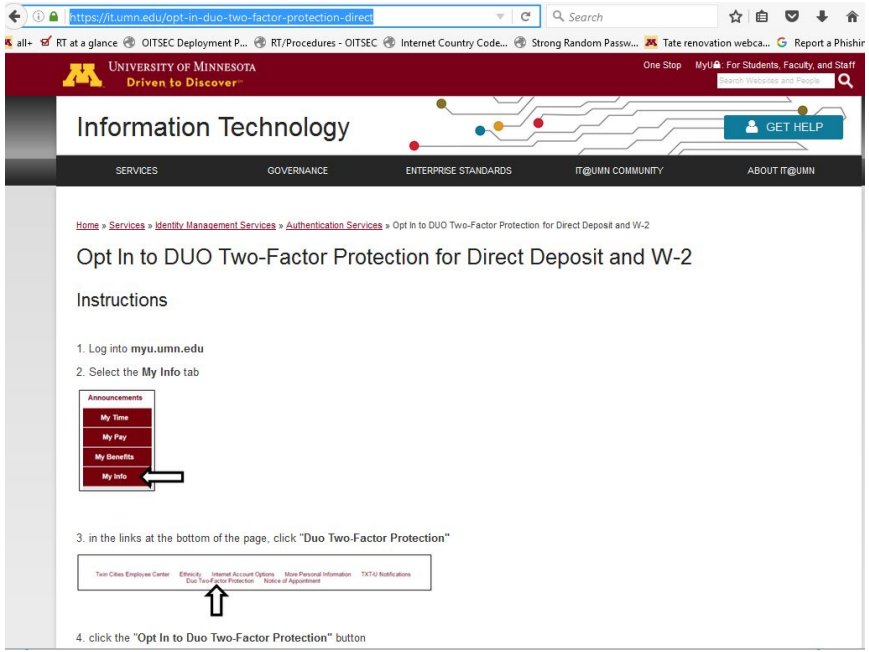
Opt In to DUO **Two-Factor** Protection for Direct Deposit and W ...
Instructions 1. Log into **myu.umn.edu** 2. Select the **My Info** tab ...
https://it.umn.edu/opt-in-duo-two-factor-protection-direct

Opt Out of Duo **Two-Factor** Protection for Direct Deposit and W ...
Instructions 1. Log into **myu.umn.edu** 2. Select the **"My Info"** tab ...
https://it.umn.edu/opt-out-duo-two-factor-protection-direct

Use Duo **Two-Factor** Protection for Direct Deposit and W-2 | IT ...
Instructions 1. Log into **myu.umn.edu** 2. Select the **"My Pay"** tab. The lin
available in the Employee Center for your campus which is accessed throug
https://it.umn.edu/use-duo-two-factor-protection-direct

Duo Push Demo using a smart phone - short video

**** Turn on 2-factor authentication everywhere you can (www.turnon2fa.com)**



IT@UMN

June 2017

Ways to stay safe online:

Strengthen your passwords

Use unique passwords for each account you create. Use passphrases or sentences. Longer = better

Keep your computers and devices up-to-date

Turn on auto-updates for operating systems and apps, even on your phone

Back Up your data - CrashPlan

In case your device is lost, stolen, or fails **+ the only real protection against Ransomware**

Be wary of scammers - don't trust your email - be suspicious and curious - ask if you are not sure!

Ask the sender via phone if you receive an unexpected attachment; get a second opinion; "Unfortunately it is the reality of the world in which we now live." (Bernard Gulachek, Interim CIO)

How strong is my password?

This is roughly how long it takes for hackers to crack passwords:

- 8 characters…... 9 minutes
- 10 characters……. 25 days
- 12 characters….. 260 years

https://howsecureismypassword.net/ to get a rough estimate of password complexity and security

IT@UMN

June 2017

Password Therapy

How passwords changed one man's life for the better: *http://www.today.com/health/how-password-changed-one-mans-life-better-1D79878606* From that article:

"Here are some of my passwords from the last 2 years, so you get an idea of how my life has changed, thanks to this method:

- Forgive@her (to my ex-wife, who started it all.)
- Quit@smoking4ever (It worked.)
- Save4trip@thailand (It worked.)
- Eat2times@day (It never worked, still fat.)
- Sleep@before12 (It worked.)
- Ask@her4date (It worked. I fell in love again.)
- No@drinking2months (It worked. I feel better.)
- Get@c4t! (It worked. I have a beautiful cat.)
- Facetime2mom@sunday (It worked. I talk with my mom every week.)

And the one for last month:
Save4@ring (Yep. Life is gonna change again, soon.)"

IT@UMN

June 2017

How do I keep track of all of my unique passwords for my buzillion accounts?

PasswordSafe
https://it.umn.edu/external/password-safe

can be used on local devices and backed up to cloud

LastPass
https://www.lastpass.com/ - cloud service

Password Management Fundamentals using LastPass
(available on Lynda.com)

IT@UMN

June 2017

What to do if you receive a telephone call, pop-up window, or email: anything that asks you to take action:

Think before you click. Try to dial back automatic behavior. Doubt and question!
This looks weird? If in doubt, reach out! Forward suspicious email or possible exposed data to:

- **abuse@umn.edu** > suspected or suspicious information security incidents
- **phishing@umn.edu** > fraudulent or suspicious email

Examples and Advisories of Scams: Phishing Blog

- z.umn.edu/phishing

Awareness Training (PJPD16) update

- All new employees are assigned
- Delivered via ulearn.umn.edu

IT@UMN

June 2017

Protect Your Mobile Devices

https://it.umn.edu/news/it-top-ten-protecting-mobile-devices

Use secure screen lock
Lock down apps too
Log out of apps
Use anti-virus
Use official app stores
Don’t install software you didn’t seek out
Don’t change default security settings or “jailbreak”
Always run updates
Use secure wifi (eduroam)
Enable remote tracking/wiping
Back up your data!

IT@UMN

June 2017

Stay Safe on the Road

https://it.umn.edu/news/secure-home-road

Use secure WiFi - password protected=more secure
Use VPN
Disable WiFi, Bluetooth, GPS if you're not using them

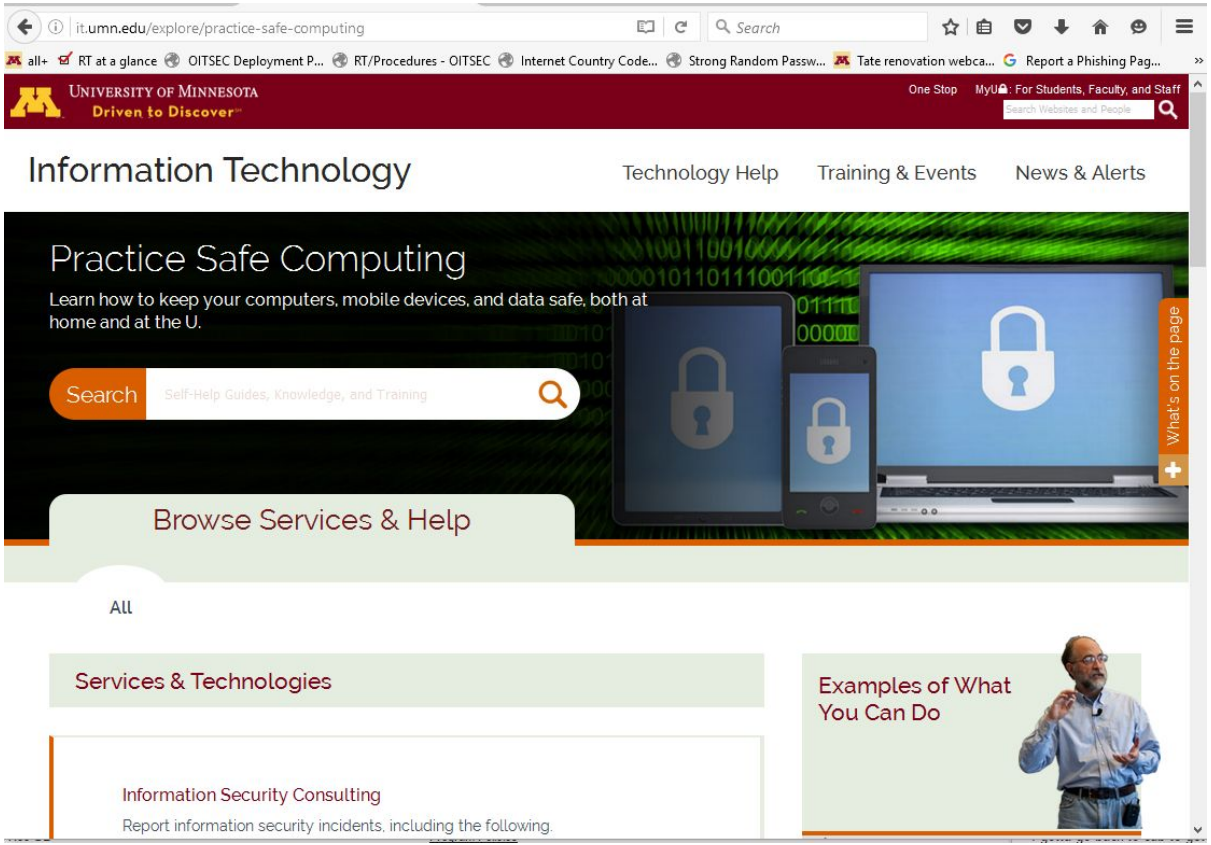
IT@UMN

June 2017

Practice Safe Computing Web site lists best practices

Be informed about steps you can take

http://safecomputing.umn.edu



Questions?
Comments? Stories?

University of Minnesota

THANK YOU

University of Minnesota